SAML2int profile v0.2.1

SAML 2.0 Interoperability Deployment Profile

1 Required Information

- Document identifier: `http://saml2int.org/profile`

2 Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119 (http://www.ietf.org/rfc/rfc2119.txt)].

The use of SHOULD, SHOULD NOT, and RECOMMENDED reflects broad consensus on deployment practices intended to foster both interoperability and guarantees of security and confidentiality needed to satisfy the requirements of many organizations that engage in the use of federated identity. Deviating may limit a deployment's ability to technically interoperate without additional negotiation, and should be undertaken with caution.

3 Introduction

This profile specifies behavior and options that deployments of the SAML V2.0 Web Browser SSO Profile [SAML2Prof (http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)] are required or permitted to rely on. The requirements specified are in addition to all normative requirements of the original profile, as modified by the Approved Errata [SAML2Err (http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf)], and readers should be familiar with all relevant reference documents. Any such requirements are not repeated here except where deemed necessary to highlight a point of discussion or draw attention to an issue addressed in errata, but remain implied.

This profile addresses the content, exchange, and processing of SAML messages only, and does not address deployment details that go beyond that scope. Furthermore, nothing in the profile should be taken to imply that disclosing personally identifiable information, or indeed any information, is required from an Identity Provider with respect to any particular Service Provider. That remains at the discretion of applicable settings, user consent, or other appropriate means in accordance with regulations and policies.

Note that SAML features that are optional, or lack mandatory processing rules, are assumed to be optional and out of scope of this profile if not otherwise precluded or given specific processing rules.

4 References to SAML 2.0 specification

When referring to elements from the SAML 2.0 core specification [SAML2Core (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)], the following syntax is used:

- `<saml2p:Protocolelement>` - for elements from the SAML 2.0 Protocol namespace.
- `<saml2:Assertionelement>` - for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specification [SAML2Meta (http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)], the following syntax is used:

- `<md:Metadataelement>`

When referring to elements from the Identity Provider Discovery Service Protocol and Profile [IdPDisco (http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf)], the following syntax is used:

- `<idpdisc:DiscoveryResponse>`

5 Metadata and Trust Management

Identity Providers and Service Providers MUST provide a SAML 2.0 Metadata document representing its entity. How metadata is exchanged is out of scope of this specification. Provided metadata MUST conform to the SAML V2.0 Metadata Interoperability Profile Version 1.0 [MetaIOP (http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf)].

Entities SHOULD publish its metadata using the Well-Known Location method defined in [SAML2Meta (http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)].

Metadata documents provided by an Identity Provider MUST include an `<md:IDPSSODescriptor>` element containing all necessary `<md:KeyDescriptor>` and `<md:SingleSignOnService>` elements. The metadata SHOULD include one or more `<md:NameIDFormat>` elements indicating which `<saml2:NameID>` Format values are supported.

Metadata documents provided by a Service Provider MUST include an `<md:SPSSODescriptor>` element containing all necessary `<md:KeyDescriptor>` and `<md:AssertionConsumerService>` elements. The metadata SHOULD also include one or more `<md:NameIDFormat>` elements indicating which `<saml2:NameID>` Format values are supported and one or more `<md:AttributeConsumingService>` elements describing the service(s) offered and their attribute requirements.

Metadata provided by Service Provider SHOULD also contain a descriptive name of the service that the Service Provider represents (not the company) in at least English. It is RECOMMENDED to also provide the name in other languages which is much used in the geographic scope of the deployment. The name should be placed in the `<md:ServiceName>` in the `<md:AttributeConsumingService>` container.

If a Service Provider forgoes the use of TLS/SSL for its Assertion Consumer Service endpoints, then its metadata SHOULD include a `<md:KeyDescriptor>` suitable for XML Encryption. Note that use of TLS/SSL is RECOMMENDED.

If a Service Provider plans to utilize a Discovery Service supporting the Identity Provider Discovery Service Protocol Profile [IdPDisco (http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf)], then its metadata MUST include one or more `<idpdisc:DiscoveryResponse>` elements in the `<md:Extensions>` element of its `<md:SPSSODescriptor>` element.

Metadata provided by both Identity Providers and Service Provider SHOULD contain contact information for *support* and for a *technical contact*. The `<md:EntityDescriptor>` element SHOULD contain both a `<md:ContactPerson>` element with a `contactType` of "`support`" and a `<md:ContactPerson>` element with a `contactType` of "`technical`". The `<md:ContactPerson>` elements SHOULD contain at least one `<md:EmailAddress>`. The *support* address MAY be used for generic support questions about the service, while the *technical* contact may be contacted regarding technical interoperability problems. The *technical contact* MUST be responsible for the technical operation of the system(s) reflected in the metadata.

6 Name Identifiers

Identity Providers MUST support the `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` name identifier format [SAML2Core (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)]. They SHOULD support the `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` name identifier format [SAML2Core (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)]. Support for other formats is OPTIONAL.

Service Providers, if they rely at all on particular name identifier formats, MUST support one of the following:

- `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`

Reliance on other formats by Service Providers is NOT RECOMMENDED.

Note that these requirements are reflected in additional constraints on message content in subsequent sections.

7 Attributes

Any `<saml2:Attribute>` elements exchanged via any SAML 2.0 messages, assertions, or metadata MUST contain a `NameFormat` of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri` .

The use of LDAP/X.500 attributes and the LDAP/X.500 attribute profile [X500SAMLattr (http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-attribute-x500-cd-01.pdf)] is RECOMMENDED where possible.

It is RECOMMENDED that the content of `<saml2:AttributeValue>` elements exchanged via any SAML 2.0 messages, assertions, or metadata be limited to a single child text node (i.e., a simple string value).

Many identity federation use cases rely on the exchange of a so-called "targeted" or "pair-wise" user identifier that is typically opaque and varies for a given user when accessing different Service Providers. Various approaches to this compatible with SAML exist, including the SAML 2.0 " `persistent` " Name Identifier format [SAML2Core (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)], the `eduPersonTargetedID` attribute [eduPerson (http://middleware.internet2.edu/eduperson/)], and the *Private Personal Identifier claim* [IMI (http://docs.oasis-open.org/imi/identity/v1.0/identity.html)].

This profile RECOMMENDS the use of the `<saml2:NameID>` element (within the `<saml2:Subject>` element), carried within the `<saml2:Subject>` with a `Format` of `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` when an identifier of this nature is required.

If an opaque targeted user identifier is being provided to the Service Provider, it is RECOMMENDED to use a `<saml2:NameID>` construct with a `Format` of `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` rather than transporting that identifier as an `<saml2:Attribute>` .

8 Authentication Requests

8.1 Binding and Security Requirements

The `<saml2p:AuthnRequest>` message issued by a Service Provider MUST be communicated to the Identity Provider using the `HTTP-REDIRECT` binding [SAML2Bind (http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)].

Identity Providers MAY omit the verification of signatures in conjunction with this binding.

The endpoints at which an Identity Provider receives a `<saml2p:AuthnRequest>` message, and all

subsequent exchanges with the user agent, SHOULD be protected by TLS/SSL.

8.2 Message Content

The `<saml2p:AuthnRequest>` message issued by a Service Provider MUST contain an `AssertionConsumerServiceURL` attribute identifying the desired response location. The `ProtocolBinding` attribute, if present, MUST be set to `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.

In verifying the Service Provider's Assertion Consumer Service, it is RECOMMENDED that the Identity Provider perform a case-sensitive string comparison between the requested `<saml2p:AssertionConsumerServiceURL>` value and the values found in the Service Provider's metadata. It is OPTIONAL to apply any form of URL canonicalization, which means the Service Provider SHOULD NOT rely on differently canonicalized values in these two locations. As an example, the Service Provider SHOULD NOT use a hostname with port number (such as `https://sp.example.no:80/acs`) in its request and without (such as `https://sp.example.no/acs`) in its metadata.

The `<saml2p:AuthnRequest>` message MUST NOT contain a `<saml2:Subject>` element.

Identity Providers that act as a proxy (per section 3.4.1.5.1 of [SAML2Core (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)]) MUST support `<saml2p:AuthnRequest>` messages that do not contain a `<saml2p:Scoping>` element.

The `<saml2p:AuthnRequest>` message SHOULD contain a `<saml2p:NameIDPolicy>` element with an `AllowCreate` attribute of "`true`". Its `Format` attribute, if present, SHOULD be set to one of the following values:

- `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`
- `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`

The `<saml2p:AuthnRequest>` message MAY contain a `<saml2p:RequestedAuthnContext>` element, but SHOULD do so only in the presence of an arrangement between the Identity and Service Providers regarding the Authentication Context definitions in use. The `Comparison` attribute SHOULD be omitted or be set to "`exact`".

9 Responses

9.1 Binding and Security Requirements

The `<saml2p:Response>` message issued by an Identity Provider MUST be communicated to the Service Provider using the `HTTP-POST` binding [SAML2Bind (http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)].

The endpoint(s) at which a Service Provider receives a `<saml2p:Response>` message SHOULD be protected by TLS/SSL. If this is not the case, then Identity Providers SHOULD utilize XML Encryption and return a `<saml2:EncryptedAssertion>` element in the `<saml2p:Response>` message. The use of the `<saml2:EncryptedID>` and `<saml2:EncryptedAttribute>` elements is NOT RECOMMENDED; when possible, encrypt the entire assertion.

Whether encrypted or not, the `<saml2:Assertion>` element issued by the Identity Provider MUST itself be signed directly using a `<ds:Signature>` element within the `<saml2:Assertion>`.

Service Providers MUST support unsolicited `<saml2p:Response>` messages (i.e., responses that are not the result of an earlier `<saml2p:AuthnRequest>` message).

9.2 Message Content

Assuming a successful response, the `<saml2p:Response>` message issued by an Identity Provider MUST contain exactly one assertion (either a `<saml2:Assertion>` or an `<saml2:EncryptedAssertion>` element). The assertion MUST contain exactly one `<saml2:AuthnStatement>` element and MAY contain zero or one `<saml2:AttributeStatement>` elements.

The `<saml2:Subject>` element of the assertions issued by an Identity Provider SHOULD contain a `<saml2:NameID>` element. The `<saml2:Subject>` element MUST NOT include a `<saml2:BaseID>` nor a `<saml2:EncryptedID>`. In the absence of a `<saml2p:NameIDPolicy>` Format attribute in the Service Provider's `<saml2p:AuthnRequest>` message, or a `<md:NameIDFormat>` element in the Service Provider's metadata, the Format of the `<saml2:NameID>` SHOULD be set to `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`.

10 Normative References

[RFC2119]
Bradner, S.,
Key words for use in RFCs to Indicate Requirement Levels,
March 1997. (http://www.ietf.org/rfc/rfc2119.txt)

[SAML2Core]
OASIS Standard,
Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0,
March 2005. (http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

[SAML2Bind]
OASIS Standard,
Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0,
March 2005. (http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)

[SAML2Prof]
OASIS Standard,
Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0,
March 2005. (http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)

[SAML2Meta]
OASIS Standard,
Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0,
March 2005. (http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

[X500SAMLattr]
SAML V2.0 X.500/LDAP Attribute Profile (http://docs.oasis-open.org/security/saml/SpecDrafts-Post2.0/sstc-saml-attribute-x500-cd-01.pdf)

[MetaIOP]
OASIS Committee
Specification, SAML V2.0 Metadata Interoperability Profile Version 1.0,
August 2009. (http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf)

[IdPDisco]
OASIS Committee
Specification, Identity Provider Discovery Service Protocol and Profile,
March 2008. (http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf)

[SAML2Err]
OASIS Approved Errata,
SAML V2.0 Errata. (http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf)

11 Non-Normative References

[eduPerson]
eduPerson & eduOrg Object Classes (http://middleware.internet2.edu/eduperson/)
[IMI]
Identity Metasystem Interoperability v1.0 (http://docs.oasis-open.org/imi/identity/v1.0/identity.html)

12 Authors' addresses

- Andreas Åkre Solberg, UNINETT, andreas.solberg@uninett.no (mailto:andreas.solberg@uninett.no)
- Scott Cantor, Ohio State University, cantor.2@osu.edu (mailto:cantor.2@osu.edu)
- Eve Maler, Sun Microsystems, eve.maler@sun.com (mailto:eve.maler@sun.com)
- Leif Johansson, Stockholm University, leifj@sunet.se (mailto:leifj@sunet.se)
- Jeff Hodges, Neustar, Jeff.Hodges@neustar.biz (mailto:Jeff.Hodges@neustar.biz)
- Ian Young, ian@iay.org.uk (mailto:ian@iay.org.uk)
- Nate Klingenstein, ndk@internet2.edu (mailto:ndk@internet2.edu)
- Bob Morgan, rlmorgan@washington.edu (mailto:rlmorgan@washington.edu)
